PWS DESIGNATOR: PWS XX00
CONTRACT: N66001-17-D-0117
TASK No: N6600118F0046
TITLE: DEFENSIVE CYBERSPACE OPERATIONS RESEARCH, DEVELOPMENT, TESTING, ENGINEERING, INTEGRATION, MAINTENANCE, AND PRODUCTION SUPPORT
DATE: 12 June 2017

1.0 SCOPE:

This Performance Work Statement (PWS) describes the contractor's support to be provided to Space and Naval Warfare Systems Center Pacific (SSC PAC), Code 58250 (Innovative Cybersecurity Engineering), to develop a distributed security operations center (SOC) for the US Navy. This SOC will include capabilities such as packet capture and analytics; large-scale data analytics; cross domain data ingest and migration; Security Information and Event Management (SIEM) integration; and malware analysis. The execution of this SOC capability (which will herein be referred to as the Defensive Cyber Operations (DCO) "DCO Enclave") will include the storage, tagging, provenance, retrieval, access, and interoperability of data across multiple domains to support the data collection and analysis required to understand what constitutes anomalous activity. This will require full lifecycle development focused on industry and government best practices to include: requirements analysis; architecture development; prototyping; software development; hardware and software integration; testing; systems engineering; network engineering; security engineering; and operations.

1.1 BACKGROUND:

The PWS describes the contractor's support to be provided to Program Executive Office, Command, Control, Communications, Computers and Intelligence (PEO-C4I) and Space and Naval Warfare Systems Center Pacific (SSC PAC), Code 58250 (Innovative Cybersecurity Engineering), to develop a distributed security operations center (SOC) for the United States (US) Navy. This SOC will include capabilities such as packet capture and analytics; large-scale data analytics; cross domain data ingest and migration; Security Information and Event Management (SIEM) integration; and malware analysis. Existing Cyber Threat requires the development of new capabilities to monitor, detect, identify, track, deter and defeat adversary, criminal and insider Cyber activities on Naval networks in a non-invasive, non-interfering manner. The Defensive Cyber Operations (DCO) Enclave is a pre-Program of Record (POR) initiative establishing the environment from which Navy DCO forces conduct network monitoring activities. The engineering and documentation of the Urgent Operational Needs Statement initiative into a PEO-C4I Program Management Warfare Office for Information Assurance and Cybersecurity (PMW 130) requires Information Systems engineering, Information Security scientific research, and Department of Defense/National Security System documentation support in order to address the growing documentation, engineering and POR establishment requirements for appropriate, on time delivery to the DCO forces.

2.0 APPLICABLE DOCUMENTS

2.1 DoDI 8500.2, Information Assurance Implementation
2.2 SPAWARINST 3090.2B and 3090.2B-M (FRCB Handbook)

3.0 TECHNICAL REQUIREMENTS

The following efforts shall use Applicable Documents 2.1 – 2.1 for guidance.

The contractor shall provide the following support as specified in further detail below:

- Provide engineering and scientific support to develop and maintain all variants of laboratory, prototype and deployed systems. This shall include support for the development and maintenance of programmatic, engineering and security documentation.
- Support research and development efforts to identify enhancements that can be incorporated in the capability lifecycle.
- Support test and evaluation, integration, and installation activities at operational sites directed by SSC-PAC.

3.1 Production Installation and Support

3.1.1 The contractor shall prepare and update installation plans and related documents for (b)(3), (b)(7)e variants supported during contract period of support (A008)

3.1.2 The contractor shall assist with the coordination of the installation planning and documentation submission to the Configuration Control Board.(A008)

3.1.3 The contractor shall assist with creating and implementing the criteria for the acceptance testing and evaluation to the Test and Evaluation (T&E) board as required for review and acceptance.(A015)(A016)(A017)(A010)

3.1.4 The contractor shall assist in the application of analysis techniques to produce specified supporting documentation for installations of equipment at corresponding sites in accordance with SSCPAC and SPAWAR policy. (A008)(A010)(A018)(A019)(A020)

3.1.5 The contractor shall provide analysis of production feasibility, operations, processes, and systems.(A0008)(A009)(A013)(A014)(A022)

3.1.6 The contractor shall assist with management of configuration control. (CDRL A005)

3.1.7 The contractor shall provide operations and maintenance support, such as troubleshooting, patching, bug fixing, and feature enhancement. (A022)

3.2 Systems Engineering Support

3.2.1 The contractor shall assist in documenting system design requirements which will accumulate throughout the system and software production. System design requirements will be collected by SSC Pacific from the stakeholders and Program Management Warfare Office for Information Assurance and Cybersecurity (PMW-130). (A009)(A013)(A014)

3.2.2 The contractor shall provide project management support to the Integrated Project Team (IPT Lead), Chief Engineer, and Assistant Program Manager and assist in the development of supporting documents such as schedules, project briefs, organization charts, and budget planning.(A005)(A006)(A015)

3.2.3 The contractor shall provide support to the SSC PAC team including the preparation, test and evaluation of deployments and Engineering Changes to correct deficiencies, and maintaining (keeping up to date) of records associated with the changes data inclusive of: (1) Schedules, (2) Progressive/special reports and supporting documentation, and (3) Plans of Action and Milestones (POA&Ms), processing project management data as received, updating project files as necessary for proper management and in time to support project schedules.(A002)(A015)(A022)

3.2.4 The contractor shall provide support to the Engineering Change Request (ECR), Certification and Accreditation (C&A), and Fleet Readiness Configuration Board (FRCB) by developing necessary engineering documentation to include system design documents, test plans, hardware/software lists, vulnerability identifications, integration plans, and installations drawings.(A015)

3.2.5 The contractor shall assist in developing, modifying and updating technical documents, and organizational metrics required for DoD, Department of the Navy (DON), Fleet Cyber Command (FCC)/C10F, Space and Naval Warfare Command (SPAWAR), Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I), SSC PAC and Program Management Warfare (PMW) 130 reports. (A022)

3.2.6 The contractor shall provide support for project management requirements by acting as technical liaisons in collaboration with stakeholders and external partners to include (b)(3), (b)(7)e (b)(3), (b)(7)e (A009)(A013)(A021)

3.2.7 The contractor shall provide test planning, document creation and revision, and future test requirements support for designated test sites for research, development, and integration testing. (A015)(A016)(A017)(A018)(A022)

3.2.8 The contractor shall participate in Cyber technology forums and exchanges to include presenting technical documents, attending roundtables, taking of notes and creation of agendas.(A006)(A007)(A013)

3.2.9 The contractor shall provide technical documentation and installation support.(A015)(A022)

3.2.10 The contractor shall provide technical input and production support by assisting with technical problems/issues and recommending alternatives. (A017)(A022)

3.2.11 The contractor shall support engineering and technical efforts necessary for production equipment layout, engineering changes, and improvements to production processes.(A022)

3.3 Cybersecurity Architecture Support

3.3.1 The contractor shall perform the following duties and responsibilities associated with the design and definition of the Defensive Cyber Operations (DCO) Enclave :

3.3.1.1 Network – Design system interfaces and ensure National Security System regulatory compliance.(A022)(A023)

3.3.1.2 Collection – Identify of data types, prioritize data retention, propose data collection nodes (A013)(A014)(A022)(A023)

3.3.1.3 Design and implement data processing architectures (A022)

3.3.1.4 Design and implement data flow methodologies(A022)

3.3.1.5 System and subsystem troubleshooting/bug fixes(A017)(A018)

3.3.1.6 Configuration control management. (A015)

3.3.2 The contractor shall support certification and accreditation processes and documentation development of the project for Risk Management Framework (RMF) Authority to Operate certification. (A015)(A022)(A023)

3.4 Scalable DCO Tool Development and Engineering

3.4.1 The contractor shall assist in the design, development, prototyping, implementation, testing, integration, configuration management, training, and maintenance of using the technologies within or compatible with the DCO Enclave Reference Architecture by providing technical recommendations and feasibility analysis and system design implementation. (A022)(A020)

3.4.2 The contractor shall support the design, development, prototyping, implementation, testing, integration, configuration management, training and maintenance of using the networking environment required for and supporting all DCO Reference Architecture tools and system components by providing technical support to government leads, engineering design and system implementation, software configuration, hardware configuration, system development, testing, installation and ongoing system support as required. (A022)(A016)(A0015)

3.4.3 The contractor shall support the development, testing, and integration of open source

(b)(3), (b)(7)e

(b)(3), (b)(7)e

applications by providing qualified subject matter experts to advise Government personnel and technicians to implement system design and lifecycle support for Information System Design, Information System Administration, Cyber Information Security Analysts, Cyber/Information Security Administrators.(A015)(A011)(A012)(A016)(A022)(A023)

3.4.4 The contractor shall assist in identifying current technology for improvements to Navy information systems for implementation within the DCO Enclave Reference Architecture as applicable to the DCO mission. In particular, subject matter experts able to provide, integrate and adapt existing or develop novel real-time and near real-time distributed systems capabilities for use in , and identify or develop data analytics techniques that can be integrated with the technologies (A022).

3.4.5 The contractor shall support documentation lifecycle management related to how developed technologies contribute to the DCO mission and are operationally viable within the DCO Enclave infrastructure and analytics architecture. (A015)(A022)

3.4.6 The contractor shall develop and execute a transition plan for the integration of prototype data analytics capabilities into the operational DCO Enclave environment, coordinate development activities in accordance with the software development lifecycle, collaborate with DCO stakeholders, provide in-depth training to SSC PAC team members and stakeholders on configuration management tools such as (b)(3), (b)(7)e

(b)(3), (b)(7)e

distributed systems, optimizing system data and computational density, stream processing, data science, and scalable analytics, and identifying optimal infrastructure and architectural components to support the DCO mission for both ashore and afloat platforms. (A022)

3.4.7 The contractor shall provide presentations, collaborating with DCO stakeholders for technical guidance on emergent packet analysis and malware prevention capabilities. (A005)(A022)

3.4.8 The contractor shall provide scalable analytics, malware analytics, tool training, and development training to SSC PAC team members and other DCO stakeholders. (CDRL A005) (CDRL A006) (CDRL A011) (CDRL A015) (CDRL A016) (CDRL A017) (CDRL A019) (CDRL A020)

3.5 Monthly Status Report: The contractor shall provide a monthly technical status report, progress report and financial report. The contractor shall produce a monthly progress report with

level of effort, cost expenditures, and status of the following Performance Work Statement tasks: (CDRL A001)

3.5.1. Personnel admin
1.Hours worked on project
2.Cybersecurity (CS) Workforce (CSWF)status
3.Travel taken

3.5.2. Documents modified, submitted, or created
1.Initial draft items
1. Guides
2. Training materials
3. Configuration items
2.Document modifications
1. Status
2. Approval submission tracking
3.Final version listing

3.5.3. Research items
1.Conference attendance
2.Emergent Tech presentations

4.0 CYBER SECURITY

Accreditation Requirements for Cybersecurity Workforce
Personnel performing under this Task Order that will require privileged access and perform CS functions in accordance with the DoD Information Assurance Workforce Improvement Program (DoD 8570.01-M, dated December 19, 2005, with Change 2 dated April 20, 2010) will be required to have or obtain training and certification in compliance with this DoD manual.

As required by DoD 8570.01-M, within six months of Task Order award personnel performing CS functions will be required to have certification. Most positions will, at a minimum, require IA Level I and II Certification for Linux and Windows OS. Specific certification requirements will be determined upon award and manning of the task positions.

4.1 The contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Cybersecurity Workforce Improvement Program. The contractor shall meet the applicable information assurance certification requirements, including:

4.1.1 DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8140series. (A001)(A024)

4.1.2 Appropriate operating system certification for information assurance technical positions as required by DoD 8140 series. (A001)(A024)

4.1.3 Upon request by the Government, the contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions. (A001)(A024)

4.1.4 Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance or cybersecurity functions. (CDRL A024)

5.0 TRAVEL

Travel requirements are anticipated for this task order. Travel will adhere to the Joint Federal Travel Regulations (JFTR). Travel shall be pre-approved by the COR.

Travel to the following locations is anticipated for this Contractor:

Location	#PERS	#TRIPS	#DAYS	PURPOSE
San Diego to (b)(3), (b)(7)e, (b)(3), (b)(7)e	1	2	3	Site survey (classified)
San Diego to (b)(3), (b)(7)e (b)(3), (b)(7)e	2	1	5	System Installation, Site Surveys, System troubleshooting
San Diego to (b)(3), (b)(7)e (b)(3), (b)(7)e	1	1	5	System Installation, Site Surveys, System Troubleshooting

6.0 GOVERNMENT FURNISHED EQUIPMENT (GFE)/INFORMATION

The government will provide access to SCI spaces, commercial and government developed software, and systems necessary for system engineering, preparing classified documentation and conducting testing. Work shall be performed utilizing GFE in government facilities located at SSC-Pacific (b)(3), (b)(7)e and/or Installation sites..

7.0 SECURITY REQUIREMENT:

7.1 SENSITIVE COMPARTMENTED INFORMATION (SCI) ACCESS

Tasking performed under this Task Order will require knowledge of SCI systems and will necessitate working with information and data classified at SCI levels, as well as having access to locations and systems with SCI level information. The information regarding Cyberspace Operations is held at the SCI and Compartmented level and by its nature is considered sensitive with very limited access. SCI access will be required by personnel to perform analysis and research in order to provide the CYBER Strategic Planning Support. The work to be performed by the contractor shall include access to SCI data, information, and spaces. SCI databases to be accessed include Joint Worldwide Intelligence Communications Systems (JWICS) and National Security Agency Networks (NSANet). The contractor shall be required to attend meetings classified at TOP SECRET SCI levels.

Tasking performed under this Task Order will require knowledge of SECRET systems, and will necessitate exposure to information up to the SECRET level, as well as having access to locations and systems with SECRET level information. The information regarding US Navy Networks may be classified and compartmented by personnel for research and analysis in order to provide the Defensive Cyber Operations (DCO) structure and tool environment engineering, architecting and execution support. The work to be performed by the contractor shall include access to SECRET data, information and spaces.

Security will be as prescribed in the DD 254 for the Task Order. Sufficient contractor's personnel assigned to this effort must possess a current Single Scope Background Investigation (SSBI). Work efforts under this contract require substantial access to SCI data and spaces. Some limited support personnel are allowed who do not require SCI clearance. Certain Key personnel require a a minimum of SECRET with TS in-process, all others require a SECRET. (CDRL A002)

7.2 OPERATIONS SECURITY (OPSEC)

OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

8.0 PLACE OF PERFORMANCE

Work shall be performed at the following locations:

SSC-PAC (b)(3), (b)(7)e
Other Government spaces as designated/required
Contractor Facility (Unclassified), all located in San Diego, California.

9.0 OTHER

9.1 ENTERPRISE CONTRACTOR MANPOWER REPORTING APPLICATION (ECMRA)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Space and Naval Warfare Systems Command (SPAWAR) via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: https://doncmra.nmci.navy.mil. Reporting inputs (from contractors) will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at

https://doncmra.nmci.navy.mil.

For purposes of ECMRA reporting, the Federal Supply Code / Product Service Code applicable to this contract/order is AC65.

Details about ECMRA can be found at NMCARS 5237.102(90) https://acquisition.navy.mil/rda/home/policy_and_guidance/nmcars.

9.2 CONTRACTOR IDENTIFICATION:

Contractor employees shall identify themselves as contractor personnel by introducing themselves or requesting that they be introduced as contractor personnel and display badges or other visible identification for meetings with Government personnel. In addition, contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

9.3 FOREIGN TRAVEL REQUIREMENTS

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the SSC Pacific foreign travel team, Topside, Building 27, 2nd Floor – Room 206 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 40 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. AntiTerrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DoD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available https://atlevel1.dtic.mil/at/, if experiencing problems accessing this website contact ssc_fortrav@navy.mil. Forward a copy of the training certificate to the previous email address or fax to (619) 553-6863, SERE 100.1 Level A Code of Conduct training is also required prior to OCONUS travel for all personnel. SERE 100.1 Level A training can be accessed at https://wwwa.nko.navy.mil. Other specialized training for specific locations may also be required; contact the SSC Pacific foreign travel team.

10.0 PERFORMANCE REQUIREMENTS SUMMARY

All deliverables shall conform to the requirements of the DD Form 1423s. All deliverables shall be delivered via email and/or on a properly labeled and identified optical disk (CD-ROM or DVD-ROM). (CDRL A001,A002, ,A025). The deliverables requirements are outlined as follows:

10.1 DELIVERABLES LIST

CDRL	Data Delivery	Requirements	Due Date
A001	Contractors Progress, Status and Management	3.5	Monthly

	Reports		
A002	Status Report (Task SCI Access List)	7.1	Weekly, as needed
A005	Presentation Material	3.1, 3.2, 3.3, 3.4	3 days prior to presentation
A006	Conference Report	3.1, 3.2, 3.3, 3.4	1 day prior to meeting
A007	Conference Minutes (Meeting Minutes)	3.1, 3.2, 3.3, 3.4.	1 day post meeting
A008	Software Installation Plan (SIP)	3.1, 3.2	As Req
A009	Software Requirements Specification	3.3	As Req
A010	Technical Report – Study/Service (Validation Report (SOVT))	3.1, 3.2	5 days post activity
A011	Software Design Description (SDD)	3.2, 3.3, 3.4	As Req
A012	Software Design Description (SDD)	3.2, 3.3	As Req
A013	Interface Requirements Specification (IRS) Engineering Master Schedule	3.1, 3.2	As Req
A014	Interface Requirements Specification (IRS)	3.2, 3.3	As Req
A015	Technical Report – Study/Service (Revisions to Existing Government Documents)	3.1, 3.2, 3.3, 3.4	As Req
A016	Hardware/Software Test Plan (Development Test Plan & Operational Test Plan)	3.1, 3.2, 3.4	2 weeks prior to activity
A017	Technical Report Study/Service (Software Test Report (Development Test Report & Operational Test Report))	3.1, 3.2, 3.4	2 weeks post activity
A018	Technical Report – Study/Service (Contract Field Support [periodic Site Survey, Monthly or Weekly])	3.1, 3.2	5 days post visit/support activity
A019	Training Materials	3.1, 3.2, 3.4	As Req
A020	Training Materials (Admin, User Guides)	3.1, 3.2, 3.4	As Req
A021	Technical Report – Study/Service (Site Survey Reports (Report after site survey, weekly))	3.3	5 days post visit/support activity
A022	Scientific and Technical Reports	3.2	As Req
A023	Schematic Block Diagrams	3.3	As Req
A024	Contractor Roster	4.0	Monthly
A025	Task Order Completion Memo	11.0	2 weeks prior to task closure

10.0 INSPECTION AND ACCEPTANCE

In-process quality assurance of contractor services shall be performed by the Contracting Officer Representative COR, (b)(6) @navy.mil SSC PAC Code 58250, (619) 553-3364 and (b)(6) @navy.mil SSC PAC Code 58250, (949)-257-2683. The contractor shall provide a Task Order Completion Memo (CDRL A025) two weeks prior to task closure.